

(b) Original classification may be extended beyond six years only by officials with Top Secret classification authority and agency heads listed in section 1-2 of the order. This extension authority shall be used only when these officials determine that the basis for original classification will continue throughout the entire period that the classification will be in effect and only for the following reasons:

(1) The information is “foreign government information” as defined by the authorities in section 1.1;

(2) The information reveals intelligence sources and methods;

(3) The information pertains to communications security;

(4) The information reveals vulnerability or capability data, the unauthorized disclosure of which can reasonably be expected to render ineffective a system, installation, or project important to the national security;

(5) The information concerns plans important to the national security, the unauthorized disclosure of which reasonably can be expected to nullify the effectiveness of the plan;

(6) The information concerns specific foreign relations matters, the continued protection of which is essential to the national security;

(7) The continued protection of the information is specifically required by statute.

(c) Even when the extension of authority is exercised, the period of original classification shall not be greater than twenty years from the date of original classification, except that the original classification of “foreign government information” pursuant to paragraph (b)(1) of this section may be for a period of thirty years.

§ 2008.7 Challenges to classification.

If holders of classified information believe that the information is improperly or unnecessarily classified, or that original classification has been extended for too long a period, they should discuss the matter with their immediate superiors or the classifier of the information. If these discussions do not satisfy the concerns of the challenger, the matter should be brought to the attention of the chairperson of the Information Security Oversight Com-

mittee. Action on such challenges shall be taken 30 days from date of receipt and the challenger shall be notified of the results. When requested, anonymity of the challenger shall be preserved.

Subpart C—Derivative Classification

§ 2008.8 Definition and application.

Derivative classification is the act of assigning a level of classification to information that is determined to be the same in substance as information that is currently classified. Thus, derivative classification may be accomplished by any person cleared for access to that level of information, regardless of whether the person has original classification authority at that level.

§ 2008.9 Classification guides.

Classification guides shall be issued by the Management Office pursuant to section 2-2 of the order. These guides, which shall be used to direct derivative classification, shall identify the information to be protected in specific and uniform terms so that the information involved can be identified readily.

Subpart D—Declassification and Downgrading

§ 2008.10 Declassification authority.

The Special Representative for Trade Negotiations is authorized to declassify documents in accordance with section 3-3 of Executive Order 12065 and shall designate additional officials at the lowest practicable level to exercise declassification and downgrading authority.

§ 2008.11 Mandatory review for declassification.

(a) *Requests for mandatory review.* (1) Requests for mandatory review for declassification under section 3-501 of Executive Order 12065 must be in writing and should be addressed to:

Attn.: General Counsel (Mandatory Review Request), Office of the Special Representative for Trade Negotiations, 1800 G Street, NW., Washington, DC 20506.

(2) The requestor shall be informed of the date of receipt of the request. This